Security Architecture and Design Documentation Guidance

LOW LEVEL DESIGN (LLD)

Version 1.4

HR CDS TT

23 June 2011

REVISION HISTORY

Name	Date	Reason For Changes	Version
HR CDS TT	04 Jun 2010	Document creation	1.0
HR CDS TT	16 September 2010	Review and update by Tiger Team	1.1
HR CDS TT	13 January 2011	Review and update by Tiger Team	1.2
HR CDS TT	3 March 2011	Review and update by Tiger Team	1.3
HR CDS TT	23 June 2011	Update by Tiger Team	1.4

ACRONYMS AND DEFINITIONS

Acronym	Definition
CCA	Covert Channel Analysis
CDS	Cross Domain Solution
DRD	Development Representation Documentation
DTLS	Descriptive Top-Level Specification
FTLS	Formal Top-Level Specification
HLD	High Level Design
LLD	Low Level Design
SFS	Security Functional Specification
SP	Security Policy

OBJECTIVES

The low level design of a system provides a description of the internal workings of the system security functions in terms of components and their interrelationships and dependencies. The low level design provides assurance that the security relevant subsystems have been correctly and effectively refined.

For each component of a security relevant subsystem, the low level design describes its purpose, function, interfaces, dependencies, and the implementation of any security enforcing functions.

Figure 1 shows the relationship of the LLD to the other topic areas described in the DRD. For medium robustness, the DTLS is not present.

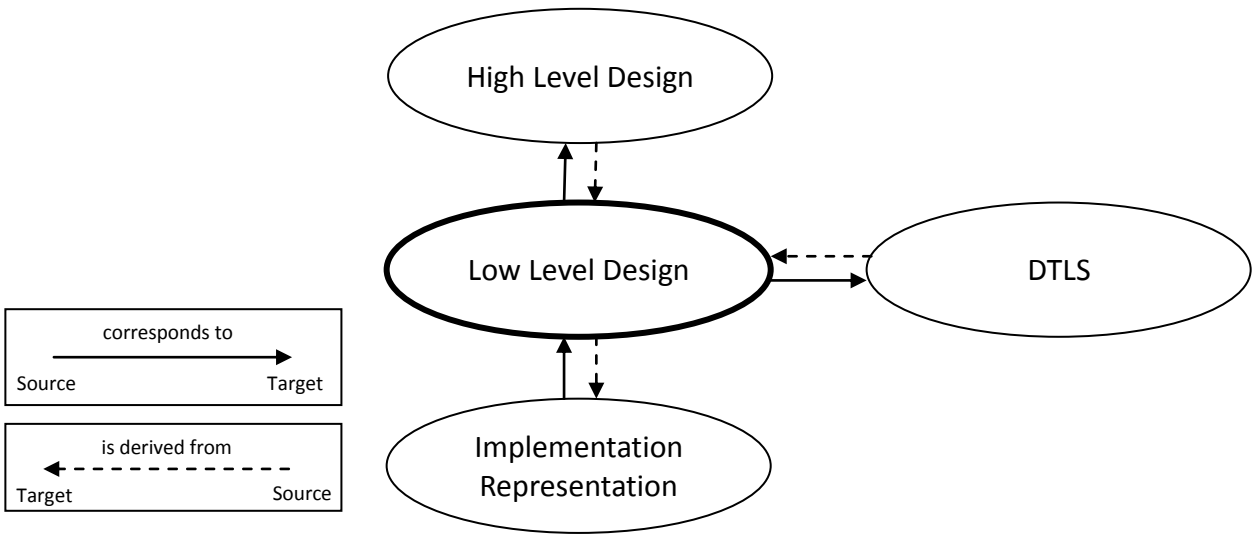

Figure 1 – Low Level Design Interactions

DISCUSSION

Design documentation typically describes two levels of decomposition: subsystem and module. A subsystem provides a high level description of what a portion of the system is doing and how. As such, a subsystem may be further divided into lower-level subsystems, or into modules. A module is the most specific design description of functionality: it is a description of the implementation.

The high level design (HLD) will typically describe one or two levels of subsystems in order to adequately convey a useful description of how the system works. The low level design (LLD) further expands the subsystem description to the module level.

The term “security functionality” represents the set of security operations that a system provides. A subsystem may provide complete security functions or may contribute to one or more security functions. This distinction is made because design constructs, such as subsystems and modules, do not necessarily relate to specific security functions. While a given subsystem may correspond directly to a security function, or even multiple security functions, it is also possible that many subsystems must be combined to implement a single security function.

The low level design shall describe how the security related functionality is provided. The intent of this requirement is that the low level design provides a description of how the design influences the implementation of each module.

REQUIREMENTS

LLD-1 The developer shall provide the low level design of the system.

LLD-2 The LLD shall be written in [selection: informal, semiformal, formal] language, as specified in the DRD.

LLD-3 The LLD shall be internally consistent.

LLD-4 The LLD shall describe the system security functions in terms of subsystems and modules.

LLD-5 The LLD shall describe the purpose of each subsystem and module.

LLD-6 The LLD shall define the interrelationships between all modules within a subsystem.

LLD-7 The LLD shall define interrelationships between modules and other subsystems.

LLD-8 The LLD shall describe each security enforcing function.

LLD-9 The LLD shall identify which of the interfaces of the system security functions are externally visible.

LLD-10 The LLD shall describe the purpose and method of use of all system security function interfaces, providing details of effects, exceptions, and error messages, as appropriate.

LLD-11 The LLD shall describe each security enforcing and security supporting function in terms of its interactions with other subsystems.

LLD-12 The LLD shall provide a mapping from the system security functions' interfaces of the functional specification to the lowest level of decomposition available in the system design.

LLD-13 The LLD shall provide a description of each module in terms of its purpose, interaction, interfaces, return values from those interfaces, and called interfaces to other modules/subsystems, supported by explanatory text where appropriate.

LLD-14 The LLD shall provide a complete presentation of the interfaces to the subsystems and modules. Such a presentation should provide the necessary detail for supporting both thorough developer and evaluator testing of the system and the assessment of vulnerabilities.

LLD-15 The LLD shall, for each security enforcing and security supporting function, identify the assumptions on inputs and assertions on outputs for the function's external interfaces.